INTRODUCTION TO KRYPTIC HUNTS

Do you exhibit great problem-solving skills? If yes, then Kryptic hunts are for you.

For as long as humans have tried to communicate, they have also made sure some of the communication stays secretive. Kryptic hunts are online scavenger hunt-style competitions where a set of clues are given and you need to bring out your inner Sherlock coupled with prodigious wit and interminable foresight to go through a series of mind-bending puzzles to reach the final answer. The internet along with all its might is at your disposal while solving this.

If you have ever wondered what the Turing machine did? or what was the text at the end of gravity falls? The answer to both these questions is an encrypted message. If I have caught your interest I suggest you try finding out the meaning behind this encryption from gravity falls.

ZHOFRPH WR FRUH

BASICS ABOUT KRYPTIC HUNTS

- All the top scorers are generally displayed on the site's leaderboard.
- The levels generally start from level 0 or level 1 and they continue in a progressive manner.
- Each Kryptic hunt has a specific duration, for 2 days or so.
- This hunt is for 48 hours.
- Usually, the hunt goes on until someone finishes the hunt or if the pre- announced time limit is over.
- This is an individual hunt and answer sharing and discussion among participants is forbidden.
- Mostly, all the hunts have unlimited tries on each level so you can try every answer that you can think of.
- There are some hunts with special formats that involve maps or tracks through which you can traverse through levels.
- Hints are released throughout the hunt whenever the admins feel they are necessary.

Learning Resources

- Many hunts have a system called Lead Confirmations - This is a certain time period in which you can ask the admins/moderators of the hunt to confirm if you are on the right track via personal messaging. https://discord.gg/BW28wXGfsZ (Discord Server Link).

DECODING MESSAGES

- In Kryptic hunt levels, there's usually some form of a message encoded within texts, images, or even audio. There are several online tools to decode these 'ciphers' or encoding.

- Sometimes, you may have to code scripts in general languages like Python to decode, this is done to make things run faster. But remember, most of it can be done manually or through existing tools.

- Google is your best friend, you shall find what you seek.

- Subtle hints may be present in discord servers, docs, intro videos, social media pages even before the hunt starts! So make sure you keep a close check on everything.

- You should check if the level text has some texts that are not visible normally. For instance, uppercase letters, underlined letters, etc forming a different word Sometimes, these clues are hidden in plain sight, with the text being of the same color as the background color.

- Hints can be present in the Page Titles as well.

This is an example of decoding a part of a level in a Kryptic hunt:

Generally, in programming languages, comments may be displayed like this

<!-- comment text --> OR   //comment text   OR   /* comment text */

You can check the source code of a website, where you'll find such comments which can be potential hints.

Shortcuts for opening the source code are-

Windows - Ctrl + U
Mac - Command + Option + U
Phone - view-source: before the URL of the website

Generally a comment looks like this –

```
<!-- I am using separate stylesheets for all three devices desktop, phone, tablet -->
<link rel="stylesheet" href="css/style1.css">
<link rel="stylesheet" href="css/style2.css">
<link rel="stylesheet" href="css/styles3.css">
```

Upon seeing this comment, you may realize that the content of it is out of the blue. It looks like an image link - a potential hint to the answer! You would want to copy and paste this URL into your browser and see for yourself what this image may hint at.

Note that it's not necessary that you'll only find a link or an image as a hint, there may be other contents, like a ciphertext waiting to be decoded or a link to something within the website.

Tools

Ciphers are well-defined instructions that help to encode or decode. Some ciphers also use keys as part of the formula. Some ciphers are - Caesar, Vigenere, Bifid, etc. You can also use certain online Cipher Identifiers when you need help identifying certain ciphers.

- [Decrypt a Message - Cipher Identifier - Online Code Recognizer](#)
- [Cipher Identifier (online tool)](#)
- [CyberChef - The Cyber Swiss Army Knife](#)
- [Cryptii](#)

Some encrypted texts or images have weird-looking symbols in them. Generally, they are some sort of symbol cipher.

Steganography refers to hiding a file within another file. This can be anything like audio, video, images, texts. You can use various websites available online to decode steganographic data.
Some helpful sites are -

https://stylesuxx.github.io/steganography/
https://www.mobilefish.com/services/steganography/steganography.php
https://manytools.org/hacker-tools/steganography-encode-text-into-image/
https://aperisolve.fr/

LSB can hide messages by using the steganography technique in which you check the Least Significant Bits of an image. You can use this website to decode messages that are encoded through the LSB technique - https://incoherency.co.uk/image-steganography/#unhide

EXIF data - (also sometimes referred to as **metadata**) contains information such as aperture, shutter speed, ISO, focal length, camera model, the date the photo was taken and much more. You can also include copyright information in your **EXIF data** when you register your camera through the manufacturer.

You can use online tools like - http://exif.regex.info/exif.cgi

Audio Files

If you have an audio file (.mp3, .wav) you can use tools like spectrum analyzer and certain steganography tools. You can also change the pitch of the audio or reverse it. Some helpful tools for this are -
Steganographic Decoder - https://futureboy.us/stegano/decinput.html
Spectrum analyzer
Sonic audio visualizer
Audacity

Links and other tools

URL Shorteners - These are special URLs that help us to use a shorter vision of the original URL. Common shorteners used in hunts are - bit.ly tinyurl.com cutt.ly
Some Kryptic hunts also have had custom shorteners like - eroc.ml quic.ml bhyi.tk

Common URLs - Some levels might have random strings in them which can be added to the back of common websites to get the right page.
Examples are - YouTube, Google products (drive, docs, slides, forms) social media (Twitter Instagram), Pastebin, Hastebin, Imgur Google Docs

eg. you find a hint "K2iuKiC", you can try it out with websites such as the above- mentioned, by just entering it in the backlink (bit.ly/backlink or bit.ly/K2iuKiC or quic.ml/K2iuKiC or docs.google.com/document/d/K2iuKiC)

- There are also certain *onion links*, which can be opened with [tor browser](#)

URL Manipulation - Sometimes you need to put certain strings as a backlink to the hunt's website itself. An example could be - kryptic-hunt.mlsakiit.com/lethifold
In this example, lethifold is the part (hint) that you will get from the level

File Manipulation -When you receive a file from a level you can open the file directly and if that doesn't work you need to make changes to that file. This includes renaming file formats to .txt .zip .jpg etc.
To display these file extensions in the file explorer -

- Select the *View tab*.
- To display the extensions, deselect *Hide extensions for known file types*. Click on OK.

Advanced

Great! You've covered the basics of solving Kryptic hunts. It's now time to dive deeper.

Inspect element allows you to see the contents of the website, you can even edit the contents temporarily. The edits are temporary and don't change the real website. You can use other developer tools such as the network tab or the console tab to try and get through the given level.
Shortcuts are -
Windows: Ctrl + Shift +
J Mac: Cmd + Opt +J

Cookies of a site - Cookies are messages that web servers pass to your web browser when you visit Internet sites. Sometimes they can have helpful information. Some levels might require you to change the contents of a certain cookie. This can be done using chrome extensions such as cookie editors.

Changing user agent - User-agent is any software, acting on behalf of a user, which "retrieves, renders and facilitates end-user interaction with web content". In some levels, you have to change the user agent to do the level. This can be done using extensions such as User-agent switcher.

Linux Some levels require you to work on other operating systems like Linux. If you don't have one, then you can work on a Vmware workstation that runs along with your main host. There are some tools that are limited to only Linux like Stegsolve, Foremost, etc which can be used to solve levels.